PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04Q 3/00, H04M 3/22

A1

(11) International Publication Number: WO 96/16515

(43) International Publication Date: 30 May 1996 (30.05.96)

(21) International Application Number: PCT/CA95/00327

(22) International Filing Date: 7 June 1995 (07.06.95)

(30) Priority Data:
08/343,854 17 November 1994 (17.11.94) US

(71) Applicant: NORTHERN TELECOM LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

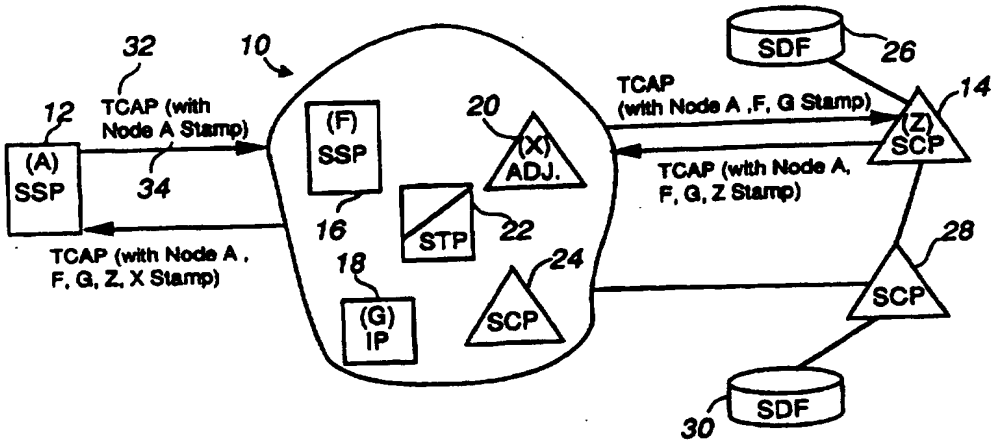
(72) Inventors: MOHARRAM, Omayma, El-Sayed; 1 Spruce Drive, R.R. #1, Carleton Place, Ontario K7C 3P1 (CA). MELNYK, Allan, Alexander; 25 Blue Meadow Way, Kanata, Ontario K2M 1L7 (CA).

(74) Agent: GRANCHELLI, John, A.; Northern Telecom Limited, Patent Dept., P.O. Box 3511, Station C, Ottawa, Ontario K1Y 4H7 (CA).

(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: INTELLIGENT NETWORK TESTING



(57) Abstract

In an Intelligent Network (IN) (10) a testing capability is provided at a service switching point (SSP) (12). The testing capability comprises a test call initiated from the SSP (12) to a desired destination (14) within the network (10). The testing capability uses network maintenance levels of signaling system number 7 (SS7) network protocol. The test call includes a message (32) sent from the SSP (12) having a portion used to log the network devices transversed in reaching the desired destination (14). The log then allows trouble shooting of the network. The testing capability helps the maintenance personnel isolate troubles and faults in the network without having to monitor each node (or office) on the route of a troubled message path.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

Intelligent Network Testing

Field of the Invention

The present invention relates to testing intelligent networks and is particularly concerned with such a capability provided at a service switching point (SSP).

Background to the Invention

An intelligent network based service requires cooperation between many different network elements and network systems. Typically an SSP and a Service Control Point (SCP) communicate using a Signaling System number 7 (SS7) network protocol. The main objective of intelligent network testing is to trouble-shoot the implementation of the SSP and SCP relevant service specifications, to ensure that they can operate harmoniously. Trouble-shooting in an operations environment where multiple network elements and the SS7 signaling network are required to set up the connection, requires either manual operations or external operations systems (OSs) to analyze and correlate the event/alert messages from the various elements in the network. Manual operations are not practical. External OSs may not be available.

When customers report trouble, or the network surveillance processes and operational systems (OSs) detect problems in the network, the tester can use the SSP maintenance capabilities to both verify and isolate these problems, and then check that they have been repaired. The SSP maintenance capabilities may include a capability to check the IN call routing and translation, a capability to access and display trigger information and status, as well as the notification (event/alert) messages and measurements. These capabilities can be used to determine the source of the problem, be it in the SSP or outside the SSP, in the remote SCP or in any other element in the network. A tester can use the SSP to launch a query to these systems, and then evaluate the responses to the query; or to verify the operation of services, old and new, after changes have been made to the network.

Further, in a multi-ventor STP and SCP operations environment, it is difficult to determine the signaling network configuration and routing of the Transaction Capability Application Part (TCAP) messages for specific subsystems. Maintenance personnel often have to rely on information given by the customer to determine the network configuration, before they start trouble-shooting the network. Capturing specific messages by setting a trap on the SSP for IN events and messages in a live environment is difficult because multiple messages from other calls and queries are coming in. This shortcoming could create the laborious task of checking the datafill at various sites in the routing message section for various multi-vendor SSPs, STPs and SCPs.

Summary of the Invention

An object of the present invention is to provide an improved intelligent network testing capability at a service switching point.

In accordance with the present invention there is provided a method of testing an intelligent network, comprising the steps of: sending a test call message including a log section from an originating node to a desired destination node via the intelligent network; at an intermediate node in the intelligent network applying its identification to the log section of the message and routing the test call message to the destination node; at the destination node, applying its identification to the log section of the test call message; and sending a return message to the originating node including the log section.

According to the invention, a service switching point (SSP) IN test call capability is provided to help isolate IN call processing failures by correlating the events and the messages generated by the SSPs, SSP-SS7 signaling and SSP-SCP/adjunct interfaces, and recording them in a log report.

Advantages of the present invention are the SSP IN network testing capability enables a tester to verify that an IN originating or terminating service, or private service

is working correctly from an individual subscriber's point of view. It also enables the tester to sectionalize IN call processing and signaling failures to the responsible IN element in the network, (i.e., SCP/Adjunct, local IP, remote IP, remote SSP). It is particularly useful for isolating intermittent IN call processing failures that are difficult and time-consuming for tester to reproduce.

Brief Description of the Drawings

The present invention will be further understood from the following description with reference to the drawings in which:

Fig. 1 illustrates testing an intelligent network in accordance with an embodiment of the invention;

Fig. 2 illustrates a CCS7 ISDNUP (ISUP) message for basic call setup;

Fig. 3 illustrates a CCS7 (IN query) message;

Fig. 4 illustrates a CCS7 maintenance message including a test call parameter (TCP) and a travelling log (TCPTLog) in accordance with an embodiment of the present invention;

Fig. 5 illustrates parameter fields for the TCP of Fig. 4;

Fig. 6 illustrates in greater detail TCP time field of parameter fields of Fig. 5;

Fig. 7 illustrates the travelling log (TCPTLog) of Fig. 4 for an originating node;

Fig. 8 illustrates the travelling log (TCPTLog) of Fig. 4 for an intermediate IN node;

Fig. 9 illustrates the travelling log (TCPTLog) of Fig. 4 for a destination node;

Fig. 10 illustrates the travelling log (TCPTLog) of Fig. 4 encoding format for a terminus node where $N > 13$.

Fig. 11 illustrates a representative network configuration including two intelligent networks to be tested in accordance with an embodiment of the present invention; and

Fig. 12 illustrates the IN test call message as it passes through the forward and return paths through the intelligent network.

Detailed Description

Referring to Fig. 1, there is illustrated testing an intelligent network in accordance with an embodiment of the present invention. The intelligent network 10 provides connection between a service switching point (SSP) 12' labeled as Node A, and a service control point (SCP) 14, labeled as Node Z. The intelligent network 10 includes nodes B through X, but for simplicity only a few nodes are illustrated and labeled. Connections between nodes within the intelligent network 10 are not shown in Fig. 1, indicative of the fact that SSP 12 (Node A) has no knowledge of such connections. Hence, the intelligent network 10 is represented by an SSP 16, labeled Node F, an intelligent peripheral (IP) 18, labeled Node G, an adjunct 20, labeled Node X, signaling transfer point (STP) 22 and an SCP 24. The SCP 14 is logically connected to a service data function (SDF) 26 and is connected to another SCP 28 having its own SDF 30.

In operation, the SSP 12, requiring connection to the SCP 14, for example for a new network service, desires testing of the connection through the intelligent network 10. In accordance with an embodiment of the present, testing is accomplished by launching a test call from the SSP 12 to the SCP 14 through the intelligent network 10. The test call is in the form of a message 32 sent from the SSP 12. The SSP 12 indicates in a log report 34 in the message its identity by including a Node A stamp. The SSP test call capability, at a given node, for example SSP 16 (Node F) determines from the test call message if the routing message is a maintenance message, then checks if the node in the routing message is its own node:

- If it matches, the SSP 16 (node F) attaches a stamp in the log report 34 section of the message, indicating that it reached the node. The node then replies to the "originating" node, SSP 12, with an appropriate

maintenance message including the log report of where the message has been.

- If it doesn't match, the SSP 16 (node F) attaches a stamp in the log report 34 section of the message 32, and forwards the message 32 according to the routing tables.
- If it doesn't match and it cannot be routed further, the SSP 16 (node F) attaches a stamp in the log report 39 section of the message 32 along with an "error indication - no route" and replies to the "originating" node, SSP 12, with an appropriate maintenance message.

The test call capability helps a tester isolate trouble and faults in the intelligent network 10 without having to monitor each node (or office) on the route of a troubled message path. The tester could access the capability locally or remotely by using a craft terminal or an operations system (OS). The test call capability provides originating, intermediate and terminating node stamps along the routing message. It also uses some maintenance levels of the CCS7 signaling network TCAP messages. These are described in greater detail hereinbelow.

The SSP 12 and SCP 14 communicate via the intelligent network 10 using SS7 network protocol.

The messages carried on the Signaling System number 7 SS7 network protocol are known as Common Channel Signaling number 7 (CCS7) messages.

CCS7 messages and telephone calls are routed in accordance with information imbedded in CCS7 messages. Two types of CCS7 messages relevant to IN test call capability are: the CCS7 ISDN User Part (ISDNUP or ISUP) and the Intelligent Network (IN) Query Message or Package.

CCS7 messages have three parts:

- Message Transfer Part (MTP) containing the routing label including the Origination Point Code (OPC) and Destination Point Code (DPC).
- Signaling Connection Control Part (SCCP) containing the Global Title information.

- Data field containing either
  - Data for call setup. The data for call set up is defined as ISDN User Part (ISDNUP or ISUP) data, or
  - Data for database services. This data is defined as Transaction Capability Application Part (TCAP) data.

All data packets (or packages) sent across the network must have the originating and terminating port addresses imbedded in the packet header. In the Signaling System number 7 (SS7) terminology these addresses are called the Originating Point Codes (OPC) and Destination Point Codes (DPC), respectively.

Referring to Fig. 2, there is illustrated a CCS7 ISDNUP/ISUP message for basic call setup. The CCS7 ISDNUP/ISUP message 40 includes the MTP 42, the SCCP 44, and the ISDNUP 46. As shown, basic call routing requires the MTP, SCCP and ISDNUP (or ISUP).

Referring to Fig. 3, there is illustrated a CCS7 IN query message. The CCS7 IN query message 50 includes the MTP 52, the SCCP 54, and the TCAP 56.

The SSP IN test call uses ISDNUP messages or TCAP messages to provide a test call parameter (TCP). The SSP, for example SSP 12 of Fig. 1, retains the TCP parameter for subsequent use for propagation and generation of log report entries during the IN test call.

The TCP is used to mark and trace test calls and activate generation and collection of the log report entries on selected calls through the intelligent network.

Referring to Fig. 4, there is illustrated a SS7 message including the TCP and log report referred to hereinbelow as travelling log (TCPTLog).

Only the parameters and fields relevant to the present embodiment are described:

A) Flag A:

Flag A unique 8 bit pattern (01111110) is used to delimit the SS7 message.

B) Backward Sequence Number (BSN) and Backward Indicator Bit (BIB): Backward sequence information is used in conjunction with forward sequence information to provide signal unit sequence control and acknowledgment functions. The sequence information is important to message flow control on the individual signaling links used to transmit SS7 messages.

C) Forward Sequence Number (FSN) and Forward Indicator Bit (FIB): Similar to BSN and BIB.

D) Length Indicator (LI):
This field indicates the number of octets contained between the length indicator octet and the error check bits. Length is indicated as a binary number. A length indicates value of 0 (code "000000") designating a fill-in signal unit. Link status signal units have a length indicator of either one or two (code "000001" or "000010"). Message signal units have length indicators greater than two. If the signaling information field of a message signal unit spans more than 62 octets, the length indicators are set to 63 (code "111111").

E) Service Information Octet (SIO):
This field contains a service indicator (bits 4-1) that indicates the Message Transfer Part (MTP)-user part involved in the message. The service indicator should be encoded with one of the following values:

bits 4321

0000 Signaling network management
0001 Standard signaling network testing and maintenance
0010 Special signaling network testing and maintenance
0011 Signaling Connection Control Part (SCCP)
0101 Integrated Services Digital Network (ISDN) User Par.

The sub-service field (bits 8-5) provides a network indicator. All messages originating from the switching system should be coded as national network messages as

indicated by code "10" in bits 8-7. Bits 6-5 are used to indicate message priority, where priority 0 is assigned to lowest priority messages. Priority 3 is the highest priority assigned to SS7 messages and is reserved for messages critical to the performance of the MTP. The priority of a message is determined by the MTP-user, and message priority should be coded as follows:

Bits 65

00 priority 0
01 priority 1
10 priority 2
11 priority 3

F) Signaling Information Field (SIF)

This is a variable length that carries the information generated by MTP-user. The format and codes for signaling information field are defined separately for each user part. The signaling information field may contain up to 272 octets of information.

G) Routing Label

The routing label consists of 3 octets for the Destination Point Code (DPC), 3 octets for Originating Point Code (OPC), and one octet for the Signaling link Selection.

H) Heading codes

Heading codes to indicate the reason for sending the signaling network management message. Heading code H0 is encoded as follows:

bits 4321

1001 TEST CALL message
1010 MTP User Flow Control messages

Code assignments for heading code H1 depend on the value assigned to H0.

J) TEST CALL Parameter (TCP)

TEST call parameter (TCP) encoding should be as shown in Fig 5. The TCP field length is 6 octets.

K) TCP Travelling Log

TCP travelling log (TCPTLog) length is 64 octets. The TCPTLog field should be encoded as detailed in Figs. 7, 8, 9 and 10.

L) Check Bits (CK)

Each signal unit has a 16 bit cyclic redundancy check field for error detection.

Called Party Address includes the following (some of):

- Called Party ID

  This parameter contains the Directory Number (DN) associated with the called party. Called Party ID is IN digit parameter range (0-15 digits)

- Called Party Station Type

  This parameter contains the station type of the called parties. The parameter value range (0...99). Existing Called Party Station Type value for TEST CALL is 95.

- Charge Number

  The Charge Number range is 0, 3, 6, 10 digits.

- Charge Party Station Type

  This parameter indicates the calling station type. The parameter value range is (0...99). Existing value for Test Call is 99.

- Global Title Value (GTV)

  This parameter contains the information included in the Global title Value (GTV) in the SCCP (Signaling Connection Control Part) Called Party Address sent for the SSP to the SCP in the SCCP Unit Data message containing the IN message.

- Calling Party Address includes the following (some of):
  - Calling Party ID
    This parameter contains the calling party number. Calling Party ID in IN digits range 3, 6, 10-15 digits.

- OPC and DPC
  - Destination Point Code (DPC)
    For SSP-to-SCP Messages, the message point code indicates which SS7 DPC (Destination Point Code) the message is going to.
    Destination Point Code identifies the intended network element/network system (e.g., intended SCP).
  - Origination Point Code (OPC)
    For SCP-to-SSP message, the message point code indicates from which SS7 OPC (Originating Point Code) the message came.
    Origination Point Code identifies the host name or address.

Referring to Fig. 5, there is illustrated parameter fields for the TCP parameter of Fig. 4. The parameter fields and values are:

- TcpDoNotAltr field 60
  TCP Do Not Alert (TcpDoNotAlert) field determines whether or not called party alerting should be performed. The TCP Do not Alert field shall be encoded as follows:
  Bit 1
  0 Alert Call
  1 Do not alert call
- TcpAMATr field 62
  TCP AMA Treatment (TcpAMATr) field defines how network AMA records should be marked for an IN Test Call. This field identifies in an AMA record that an IN call or portion of an IN call (e.g., IN portion) is part of a test call. This field shall be encoded as follows:

Bit 2

0 Do not mark AMA record as part of Test Call

1 Mark AMA record as part of Test Call

- TcpTLogLev field 64

TCP Travelling Log level (TcpTLogLev) field determines whether or not T-Log entries to be generated in the travelling log section of the IN Test Call message (TCPTLog). This field shall be encoded as follows:

Bits 43

00 T-Log entry not requested

01 Generate time-stamped IN Test Call-related entry in the TCPTLOG

10 Generate time-stamped IN Test Call-related entry in the TCPTLog and IN NE/NS internal log message

11 Generate time-stamped IN NE/NS internal messages.

- TcpTLogRepInd field 66

TCP Travelling Log Report Indicator (TcpTLogRepInd) field specifies how the T-Log records are to be reported. This field shall be encoded as follows:

Bit 5

0 Automatically report T-Log entries to the Originating point code (OPC)

1 Store T-Log entries in internal message and report them to the OPC when requested.

- TcpTLogID field 70

TCP Travelling log ID (TcpTLogID) field identifies the travelling log relevant to a specific IN service test call-related messages and data. This field shall be a two (2) octet integer that identifies a T-Log. The most significant octet is (00000000) when the TCP T-Log ID is less than 256 .

- TCPTime field 72

TCP Time (TcpTime) field specifies the artificial time data and date that SCP/Adjunct service logic should use when processing the IN TEST CALL. This field contains

the following fields: TCP Null Indicator, TCP Time Year, TCP Time Month, TCP Time Date, TCP Time Hour, TCP Time Minute. This field shall be encoded as illustrated in Fig. 6 and described hereinbelow.

- The TCP Time Year field should be encoded as follows:

Bits 21 (in the 1st Octet in Fig. 6)

00	0 (last)
01	1 (current)
10	2 (next)
11	Spare

- The TCP Time Month field should be encoded as follows:

Bits 6543 (in the 1st Octet in Fig. 6)

0000	Spare
0001	January
0010	February
0011	March
0100	April
0101	May
0110	June
0111	July
1000	August
1001	September
1010	October
1011	November
1100	December
1101	Spare
1110	Spare
1111	Spare

- The TCP Time Null Indicator field should be encoded as follows:

Bits 87 (in the 1st Octet in Fig. 6)

11	Null
01	Not Null
10	Reserved
11	Reserved

- The TCP Time Date field should be encoded as follows:

Bits 54321 (in the 2nd Octet in Fig. 6)

00000	Spare
00001	1
00010	2
00011	3
00100	4
00101	5
00110	6
00111	7
01000	8
01001	9
01010	10
01011	11
01100	12
01101	13
01110	14
01111	15
10000	16
10001	17
10010	18
10011	19
10100	20
10101	21
10110	22
10111	23
11000	24
11001	25
11010	26
11011	27
11100	28
11101	29
11110	30
11111	31

- The TCP Time Hour field should be encoded as follows:

Bits 54321 (in the 3rd Octet in Fig. 6)

00000	0
00001	1
00010	2
00011	3
00100	4
00101	5
00110	6
00111	7
01000	8
01001	9
01010	10
01011	11
01100	12
01101	13
01110	14
01111	15
10000	16
10001	17
10010	18
10011	19
10100	20
10101	21
10110	22
10111	23
11000	Spare
11001	Spare
11010	Spare
11011	Spare
11100	Spare
11101	Spare
11110	Spare
11111	Spare

- The TCP Time Minute field should be encoded as follows:

Bits 76 (in the 3rd Octet in Fig. 6)	
00	0 minutes
01	15 minutes
10	30 minutes
11	45 minutes

This field identifies the nearest quarter-hour.

Other fields may be added to the TCP for easy identification of the Test Call and Travelling log. Some of these parameters may be as follows:

- TCP Travelling Log name (TcpTLog Name) associates a logical name with a TCPTLOG.
- TCP Travelling Log serial Number (TcpTLogSerialNo) field uniquely identify the TCPTLog.
- TCP Travelling Log sequence Number (TcpTLogSeqNo) field allows T-Log records to be sequentially maintained across multiple IN network elements (NEs) and network systems (NSs) where the internal clocks of such systems may not be synchronized. The sequence number maintains T-Log entries in their correct sequence across IN NEs/NSs. TcpTLogSeqNo range (0... 65535).
- TCP Service Provider ID (TcpSvcProvId) field identifies the service provider responsible for IN network Test Call.
- TCP Call Progress Indicator (TcpCalled PrgInd) field provides service-specific call progress reports during an IN Test Call.
- TCP Test request indicator (TcpTLogRepInd) field determines whether or not a service-specific test is performing during an IN Test Call.
- TcpTLog field 74
  Details of the TLog given hereinbelow in conjunction with Fig. 4.

Figs. 7 - 10 illustrate the format used for the travelling log TCPTLog field of Fig. 4.

Fig. 7 shows the travelling log encoding format at the originating node, that is the SSP IN node where the IN Test Call is launched, for example SSP 12 in Fig. 1.

Fig. 8 shows the additional information that an intermediate IN node would add to the travelling log. The length of the information is typically 4 octets (3 octets to identify the IN node PC and one octet of information).

At the end of the first leg of the IN Test Call, the node adds to the travelling log section 8 octets as shown in Fig. 9.

The first 4 octets identify the node PC and the function information in terms of route selection and availability/usability. The second 4 octets identify the PC at the first leg end of the Test Call an "all one's flag" and normal operation Fault Code (TcpFaultCode is 0).

Fig. 10 shows the travelling log encoding format when the number of nodes in the IN Test Call Travelling Log exceeds 13 nodes. The limit of 13 nodes (or 13 log entries) resulted from the 64 Octets travelling log length imposed in the present embodiment.

It is assumed that the travelling log has a fixed 8 octets of overhead (the 1st 8 octets of Fig. 7). The travelling log length for the intermediate nodes and the terminus node is 56 octets. Since each node is allowed 4 octets of log entries, the total number of points is 14 (56/4). But the terminus node is allowed additional 4 octets for End Flag and Fault code log entries. Therefore, the maximum number of the 4 octets log entries is 13. The 13 points (or nodes) of log entries include the log entries from the originating node, the intermediate nodes and the destination or terminus node. If the travelling log length were increased (that is, greater than 64 octets), the number of log entries points (or nodes) would increase accordingly.

If the number of log entries points exceeds 13 (N>13) the travelling log entries fields should be encoded as shown in Fig. 10.

Referring to Figs. 7-10, the travelling log field values are as follows:

- TcpMsgID field 80
  The TCP message identifier is 8 bits length
- TcpRouteSelection 82
  The TCP route selection is function of the route COST (least cost or high cost), route engineered (or provisioned) and route usability per node (or office).
  The Least and High cost selection should be encoded as follows:
  - 00 No Cost criterion
  - 01 Least Cost
  - 10 High Cost
  - 11 Not Valid.

  The route availability and usability selection should be encoded as follows:
  - 00 Choose any route
  - 01 Choose selected cost if usable, otherwise choose any route
  - 10 Choose selected cost if usable, otherwise fail
  - 11 Reserved

  Therefore, the TCP Route Selection (TcpRouteSelection) field should be encoded as follows:

  Bits 4321 (in the 2nd Octet in Fig. 7)
  - 0000 Choose any route
  - 0001 Error
  - 0010 Error
  - 0011 Error
  - 0100 Error
  - 0101 Choose least cost if usable, otherwise choose any route
  - 0110 Choose high cost if usable, otherwise choose any route
  - 0111 Error

1000	Error
1001	Choose least cost if usable, otherwise fail
1010	Choose high cost if usable, otherwise fail
1011	Error
1100	Spare
1101	Spare
1110	Spare
1111	Spare

Accordingly, the node may choose one of the following routes:

a. Route 1: Any Route

b. Route 2: Least cost if available and usable, otherwise choose any route

c. Route 3: High cost if available and usable, otherwise choose any route

d. Route 4: Least cost if available and usable, otherwise fail

e. Route 5: High cost if available and usable, otherwise fail.

If the node route selection was either (1001) or (1010) the IN Test Call message may fail to reach the Destination Point Code (DPC). Because if the route (Least/High cost) is not available and usable in the network everywhere along the IN Test Call message route (i.e., end-to-end, OPC to DPC) the test will fail.

- TcpDirInd 84

The TCP Direction Indicator field identifies the message direction relative to the originating node. One bit is used to identify the Forward direction 1 and Reverse direction 0.

Bit 5	(in the 2nd Octet in Fig. 7)
0	Forward Direction
1	Reverse Direction

- Destination Point Code (DPC) 86

  The message point code indicates to which SS7 DPC (Destination Point Code) the message is going. DPC identifies the intended network element/network system (e.g. intended SCP). The DPC field is 3 Octets in length.

- Origination Point Code (OPC) 88

  The message point code indicates from which SS7 OPC (Originating Point Code) the message came. OPC identifies the host name or address. The OPC field is 3 Octets in length.

- TcpINNodePC field 90

  TCP IN Node ID field identifies the IN nodes (i.e. NE/NS) that is the requester of the IN Test Call. This field identifies the IN system that supplied the TCP parameters. Permissible values are:

  - For SSPs, the SS7 Point Code (PC)
  - For SCPS, the SS7 Point Code (PC)
  - For IPs, the IP ID (i.e., DN, Nature of number, Numbering Plan).

  TcpINNodePc field is 3 Octets in length.

- Tcp Route Usable Counter 92

  The TCP route usable counter field contains the number of usable routes in the network for the IN Test Call. The counter is 3 bits and its value ranges from 0 (zero) to 7 route usable.

- TCPRouteEngCounter 94

  The TCP Route Engineered counter field contains the number of Engineered (or provisioned) Route in the network. The counter is 3 bits and its value ranges from 0 (zero) to 7 routes Engineered (or provisioned at the node (or office)).

- TcpSelectedRouteCost 96

  The TCP selected route cost field contains the route cost selected by the IN Test Call message.

- Tcp First Leg EndPC 98

The TCP First Leg End (FLE) point code indicates the node point code at the end of the IN Test Call message path. The TcpFirstLegEndPC field is 3 Octets in length. The TcpFirstLegEndPC will always be the all one's Point Code (PC) that is, ("FF FF FF").

- TcpFaultCode 100

TCP fault code specifies the fault code. The TCP fault code is integer value with range (0... 255). The following are examples of fault code values and the relevant fault.

Message	Value
Normal	0
Time-out	2
Resource Cancelled	3
Failure	8
Channels Busy	9
Resource Not Available	11
Abort	18
Looping	23
Spare	24-255

- TcpCounter 101

The TCP Counter field contains the number of nodes in the network that the IN Test Call is travelled to without recording any information. This counter is incremented when the TCPTLog length is exhausted. The TCP Counter is 6 bits in length and its value ranges from (0... 63).

A more detailed description of the operation of the SSP IN test call is provided in conjunction with Figs. 11 and 12.

Referring to Fig. 11, there is illustrated a representative network configuration. The network configuration includes two intelligent networks labelled as Network A and Network B. The nodes of networks A and B are labelled in accordance with IN point code (PC) convention. The network A includes primary layer STP pairs 102 and 104

(having PC component 121), secondary level STP pairs B-link quad 106 including STP pairs 108 and 110 (having PC component 101) and STP pairs 112 and 114 (having PC component 103). The network A also includes an originating switch, SSP 116, (having PC component 1, PC = 245-103-001) and a second switch, SSP 118 (having a PC component 1, PC = 245-101-002). Other IN components in the network A include an SSP 120, an adjunct 122, an SSP 124, a calling party 126 is shown connected to the originating switch 116 as is an intelligent peripheral (IP) 128.

The network B includes primary layer STP pairs 130 and 132 (having a PC component 131) that together with STP pairs 102 and 104 of network A form a B-link quad 134 and a secondary level STP pairs B-link quad 136 includes STP pairs 138 and 140 (having PC component 111, PC = 252-111-150) and STP pairs 142 and 144 (having PC component 113, PC = 252-113-150). The network B also includes a serving SCP 146 (having PC component 015, PC = 252-113-015), a second SCP 148 (having PC component 016) and a terminating switch, SSP 150 (having PC component 017, PC = 252-113-017). The SSP 150 has a called party 152 connected to it. The network B1 also includes a second SSP 154 connected to the STP pairs 138 and 140.

With regard to the IN test call in accordance with the present embodiment fields of most interest are those containing information on the message route selection (TcpRouteSelection), message direction (TcpDirInd) and Travelling Log (TLog) entries section. Other fields are relevant to the CCS7 network protocol (MTP, SCCP, and TCAP) generally.

The travelling log (TLog) entries section is used to keep track of how the message propagated through the network. Based on the route selection and message direction (TcpRouteSelection and TcpDirInd), the IN test call query message will travel through the network from originating node, SSP 116 to destination node SCP 146. Ultimately, the message should find its way through to the DPC that it was

attempting to reach. However, it may not due to various error conditions in the network. As described hereinabove, The TLog section consists of a number of log entries with each entry consisting of the node Point Code (PC) and the node data.

The PC is that of the node making the log entry in the TLog section. The node data is an information field describing the condition at the node based on the requirements of the route selected by the node, the number of routes engineered (or provisioned) at the node and the number of routes usable for the IN query message at the node.

Numerous scenarios are possible for the message traversing the network. Examples of some scenarios are described hereinbelow. Four scenarios are used to further describe basic operation along a route. For the sake of presentation in the points below, the DPC designation is interchangeable with OPC based on the message direction indicator (TcpDirInd). The process is basically the same except at the end points, that it, at the DPC, the message is turned around and at the OPC, the message is analyzed.

Four scenarios that are described are:

- Successful IN test call propagation;
- Successful IN test call delivery;
- Unsuccessful IN test call delivery; and
- Unsuccessful routing.

The node receiving the test call query is not the final DPC but is successfully able to route the IN test call query to next node.

At any intermediate IN node in the network, for example STP 102, the intermediate IN node appends a log entry to the TLog section that includes its PC and includes with the log entry the result.

In the result, the TcpRouteEngCounter provides the number of routes provisioned at the node. The TcpRouteUsableCounter provides the routes available/usable

for routing the query to the next node in the query message path.

For example, if the node has selected "Route_2/Route_3, the result contains an indication of which cost was chosen and the number of routes usable for routing the query to the next node in the query message path. If there is only one route, then no cost is identified and the number of routes available is set to 1 and routes usable is set to 1. If no cost can be identified (i.e. in case of STPs load sharing) then no cost is set and routes engineered and usable are set accordingly.

Alternatively, if the node has selected Route_4/Route_5 and if the specified cost is available, then the result contains a cost indication and the routes engineered and usable.

If there is only one route and it is available/usable, then the cost is indicated and only 1 route is available/usable.

If the specified cost is not usable, then this is an error condition relating to unsuccessful routing as described hereinbelow.

The node receiving the test call query is the final DPC and is successful in handling the request.

The following activities are performed at the destination node with the destination point code (DPC), that is, SCP 146 in Fig. 11.

Fig. 12 illustrates a portion of the query as it traverses nodes in the network.

The destination node:

1. Appends a log entry 200 to the TLog section that has the PC of the DPC (015);
2. Clears the result because this is the "end of journey";
3. Includes in the log entry, a special result indication;
4. Marks the First Leg End field. This is a special log entry and it consists of an "all one's PC - FF

FF FF code along with a normal operation fault code (i.e., TcpFault Code=0);

5. Sets TcpDirInd to indicate that the message is heading in the reverse direction (e.g., TcpDirInd=1); and

6. Sends the maintenance message back towards the originating node with the originating point code (OPC).

The first leg end (FLE) indicator is used to formally mark the TLog section. This helps the system handle unexpected conditions in a logical fashion. It also provides a place to associate a TcpFaultCode in the TLog while keeping each log entry a fixed length. Unexpected events can occur along a message route at any time and for a number of reasons. The purpose of the system is to handle these conditions logically so that the problem can be sectionalized and looked at more closely with other tools or methodology.

The indicator in the TLog for direction (TcpDirInd) is used to indicate which way the message is currently propagating through the network. With reference to the originator of the IN test call query message, TcpDirInd is not set in the OPC to DPC direction. If it makes it to the DPC or there is a failure along the route, then the TcpDirInd is set.

The third scenario is the unsuccessful test call delivery. The node is the final DPC for the IN test call query message and is unsuccessful in handling the request.

The following activities are performed by the node with the destination point code (DPC):

1. Appends a log entry to the TLog section that has the PC of the DPC;

2. Clears the results because this is the "end of journey";

3. Includes in the log entry, a special result indication;

4. Marks the special First Leg End (FLE) log entry. The special log entry consists of the "all one's PC - FF FF FF" coding along with the TcpFaultCode; and

5. Sets TcpDirInd to indicate that the message is heading in the reverse direction (i.e. TcpDirInd=1).

The fourth scenario is unsuccessful routing. Unsuccessful routing can occur at various stages of the query message path. The node, unable to route the query message, must undertake the actions to identify the relevant problem to the far end.

The conditions such as route set unusable, maintenance, processor outage, may be the cause of unsuccessful routing.

The following activities are performed by the node:

1. Appends a log entry to the TLog section with its PC;

2. Includes with the log entry a result with the following indications set:

   a. If the failure was caused by not being able to route due to the actions indicated in the route selection, then cost indication in (TcpSelected Route) should be that of the route selected (i.e. least cost "01" or high cost "10") and the number of routes engineered in the (TcpRouteEngCounter) should be equal to the number of routes usable, while the routes usable counter (TcpRouteUsableCounter), should indicate the number of usable routes not meeting the cost selection.

   b. If the failure was caused by other conditions, then no cost indication should be set and the routes provisioned should be set accordingly, while routes usable should be set to 0.

c. Marks the First Leg End. As before, this is a special log entry and it consists of a PC (i.e., "all one's PC - FF FF FF) along with the error code (TcpFaultCode).
The TcpFault Code indicates that the node was unable to meet the node route selection requirements; and

3. Sets TcpDirInd to indicate that the message is heading in the reverse direction (i.e. TcpDirInd = 1).

Return of a maintenance message to the originating switch, SSP 116 of Fig. 11, indicates test completion. The return maintenance message is analyzed to see if it transversed the network without problems.

1. If there is no FLE with an TcpFaultCode (i.e. not "all ones", then the test was a success. However, the TLog is then analyzed to see if the route traverse was as expected and that there were not any unusual characteristics, such as:
   a. Unexpected PCs.
   b. Too many nodes in route.
   c. Only 1 available route.
   d. Only 1 usable route.
   If unusual characteristics are found, the user could execute a different function information arrangement (e.g. choose a different cost to force a different path);
2. If there is an FLE with a TcpFaultCode (i.e. not zero) (TcpFaultCode $\neq$ 0), then the test has discovered a potential problem. The TcpFaultCode has to be analyzed along with the return route data to sectionalize the fault to a given node and problem; and
3. Route information from the TLog can be reviewed to determine additional testing.

WHAT IS CLAIMED IS:

1. A method of testing an intelligent network (10), comprising the steps of:

sending a test call message (32) including a log section from an originating node (12) to a desired destination node (14) via the intelligent network (10);

at an intermediate node (16) in the intelligent network (10) applying its identification to the log section of the message (32) and routing the test call message (32) to the destination node;

at the destination node (14), applying its identification to the log section of the test call message; and

sending a return message to the originating node (12) including the log section.

2. A method as claimed in claim 1 wherein the originating node (12) is a service switching point.

3. A method as claimed in claim 1 wherein the intermediate node (16) includes all nodes traversed between the originating node (12) and the destination node (14).

4. A method as claimed in claim 1 wherein the step of sending a test call message (32) includes applying an identification of the originating node (12) in the log section.

5. A method as claimed in claim 1 wherein the step of routing the test call message (32) at the intermediate node (16) includes the steps of comparing the destination node identification to its own identification and, if the identifications match, completing the steps of the destination node (14).

6. A method as claimed in claim 1 wherein the step of routing the test call message (32) at the intermediate node (16) includes the step of appending to the log section (34) an indication of routes provisioned at the intermediate node (16).

7. A method as claimed in claim 1 wherein the step of routing the test call message (32) at the intermediate node (16) includes the step of appending to the log section an indication of routes available for routing the message (32) to a next node in routing the test call message.

8. A method as claimed in claim 1 wherein the step of sending a return message includes the step of appending an indication of message direction (84).

9. A method as claimed in claim 1 further comprising the step of analyzing the log section at the originating node (12) to determine whether or not problems were encountered in the intelligent network (10).

10. A method as claimed in claim 1 wherein the step of sending a return message includes, for a successful test, appending an indication of a successful completion of the route to the destination node (14).

11. A method as claimed in claim 1 wherein the step of sending a return message includes, for an unsuccessful test, appending an indication of a fault at the destination node (14).

12. A method as claimed in claim 1 wherein the test call message (32) is a common channel signaling system number 7 (CCS7) ISDN user part (ISDNUP) message.

13. A method as claimed in claim 1 wherein the test call message (32) is a common channel signaling system number 7 (CCS7) IN query message.

14. A method as claimed in claim 1 wherein the return message is a common channel signaling system number 7 (CCS7) ISDN user part (ISDNUP) message.

15. A method as claimed in claim 14 wherein the test call message (32) is a common channel signaling system number 7 (CCS7) IN query message.

16. A method of testing an intelligent network (10) comprising the steps of:

sending a test call message (32), including a log section, from an originating nodes (12) to a desired destination node (14) via the intelligent network (10);

at an intermediate node (16) in the intelligent network (10) determining the destination of the test call message (32), from routing information therein, and applying its identification to the log section; and

if the test call message (32) cannot be routed to the destination node (14), appending to the log section an indication of a cause of failure to route and sending a return message to the originating node (12) including the log section from the test call message (32).

17. A method as claimed in claim 1 further comprising the step of analyzing the log section at the originating node (12) to determine the cause of failure to route.

18. A method as claimed in claim 16 wherein the test call message (32) is a common channel signaling system number 7 (CCS7) ISDN user part (ISDNUP) message.

19. A method as claimed in claim 16 wherein the test call message (32) is a common channel signaling system number 7 (CCS7) IN query message.

20. A method as claimed in claim 16 wherein the return message is a common channel signaling system number 7 (CCS7) ISDN user part (ISDNUP) message.

21. A method as claimed in claim 16 wherein the test call message (32) is a common channel signaling system number 7 (CCS7) IN query message.

22. A method as claimed in claim 1 wherein the log section includes a test call parameter identifier field (80).

23. A method as claimed in claim 22 wherein the log section includes a test call parameter route selection field (82).

24. A method as claimed in claim 23 wherein the log section includes a test call parameter direction indicator field (84).

25. A method as claimed in claim 24 wherein the log section includes an origination point code (88) for the originating node.

26. A method as claimed in claim 25 wherein the log section includes a destination point code (86) for the destination node.

27. A method as claimed in claim 26 wherein the log section includes a test call parameter IN node identifier field (90).

28. A method as claimed in claim 27 wherein the log section includes a test call parameter route usable counter field (92).

29. A method as claimed in claim 28 wherein the log section includes a test call parameter route engineered counter field (94).

30. A method as claimed in claim 29 wherein the log section includes a test call parameter route cost field (96).

31. A method as claimed in claim 1 wherein the intermediate node identification includes an IN node identifier field.

32. A method as claimed in claim 31 wherein the intermediate node identifier includes a route usable counter field.

33. A method as claimed in claim 32 wherein the intermediate node identifier includes a route engineered counter field.

34. A method as claimed in claim 33 wherein the intermediate node identifier includes a selected routed cost field.

35. A method as claimed in claim 1 wherein the destination node identification includes a route usable counter field.

36. A method as claimed in claim 35 wherein the destination node identification includes a route engineered counter field.

37. A method as claimed in claim 36 wherein the destination node identification includes a selected routed cost field.

38. A method as claimed in claim 37 wherein the destination node identification includes a test call parameter first leg end point code field.

39. A method as claimed in claim 38 wherein the destination node identification includes a test call parameter fault code.

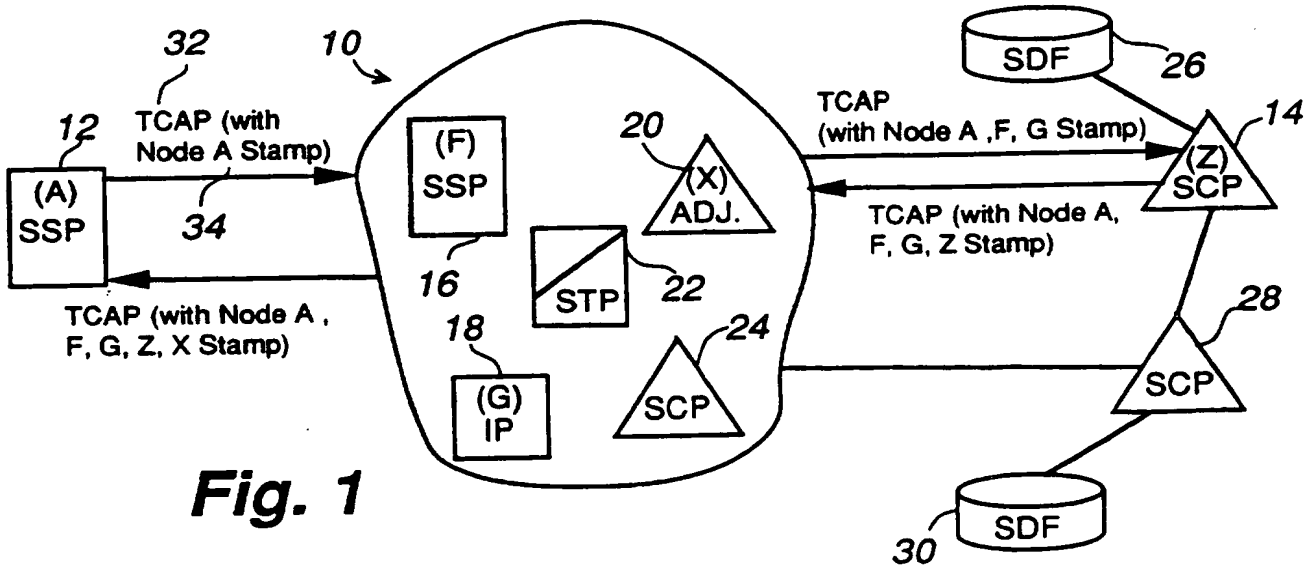


Fig. 1

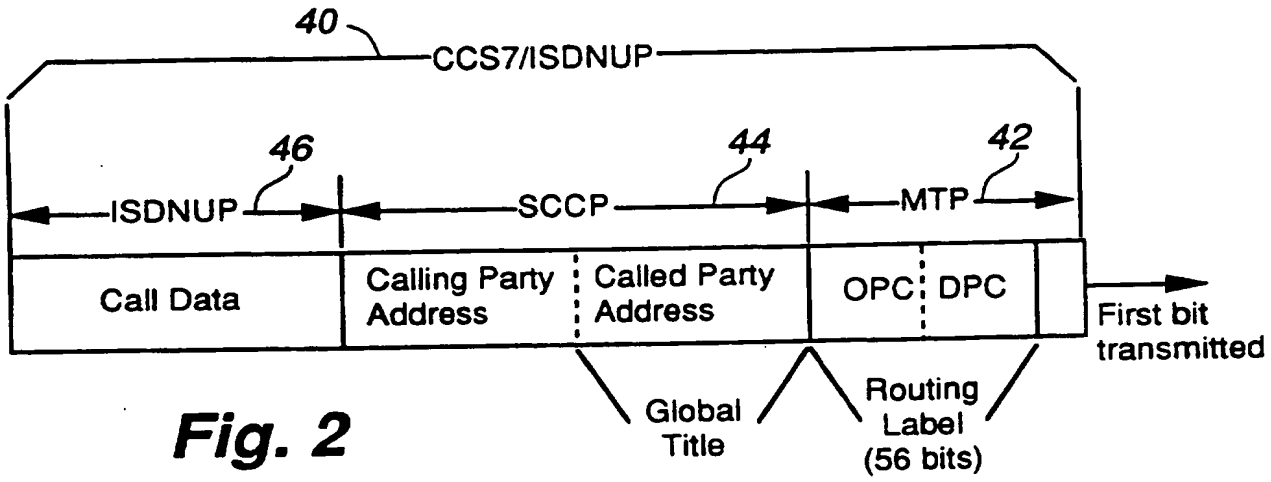


Fig. 2

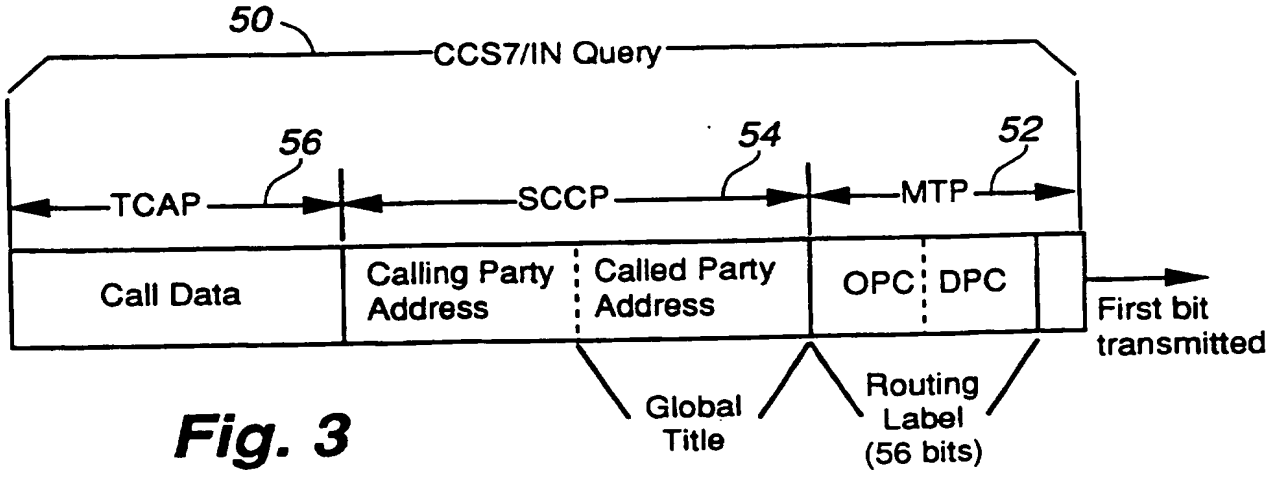


Fig. 3

		8	7	6	5	4	3	2	1	
1 Octet	A	0	1	1	1	1	1	1	0	First bit transmitted
1 Octet	B	BIB	Backward Sequence Number (BSN)							
1 Octet	C	FIB	Foreward Sequence Number (FSN)							
1 Octet	D	Spare	Length Indicator (LI)							
1 Octet	E	0	1	1	1	1	1	1	0	
										Routing Label (7 Octets)
3 Octet		Destination Point Code (DPC)								
	G									
3 Octet		Originating Point Code (OPC)								
1 Octet		Signaling Link Selection								
1 Octet	H	H1				H0				
9 Octet		Called Party Address								
8 Octet		Calling Party Address								
		Additional Information								Call Data
6 Octet	J	Test Call Parameter (TCP)								
64 Octet	K	TCP Travelling Log (TCPTLog)								
		Additional Information								
-2 Octet	L	Check Bits								

F (272 Octets)

Fig.4

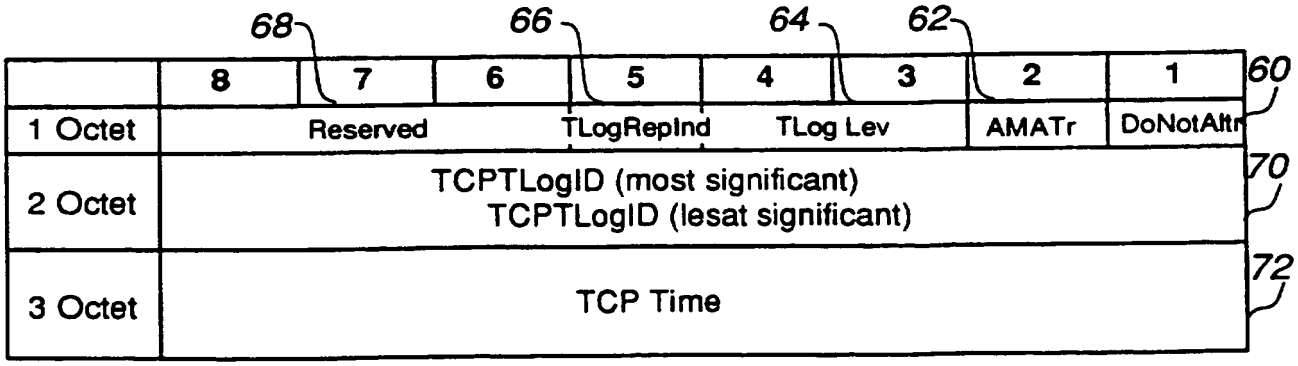


Fig.5

	8	7	6	5	4	3	2	1
1 Octet	Null Ind		Month				Year	
1 Octet	Spare			Date				
1 Octet	Spare	Minute		Hour				

Fig. 6

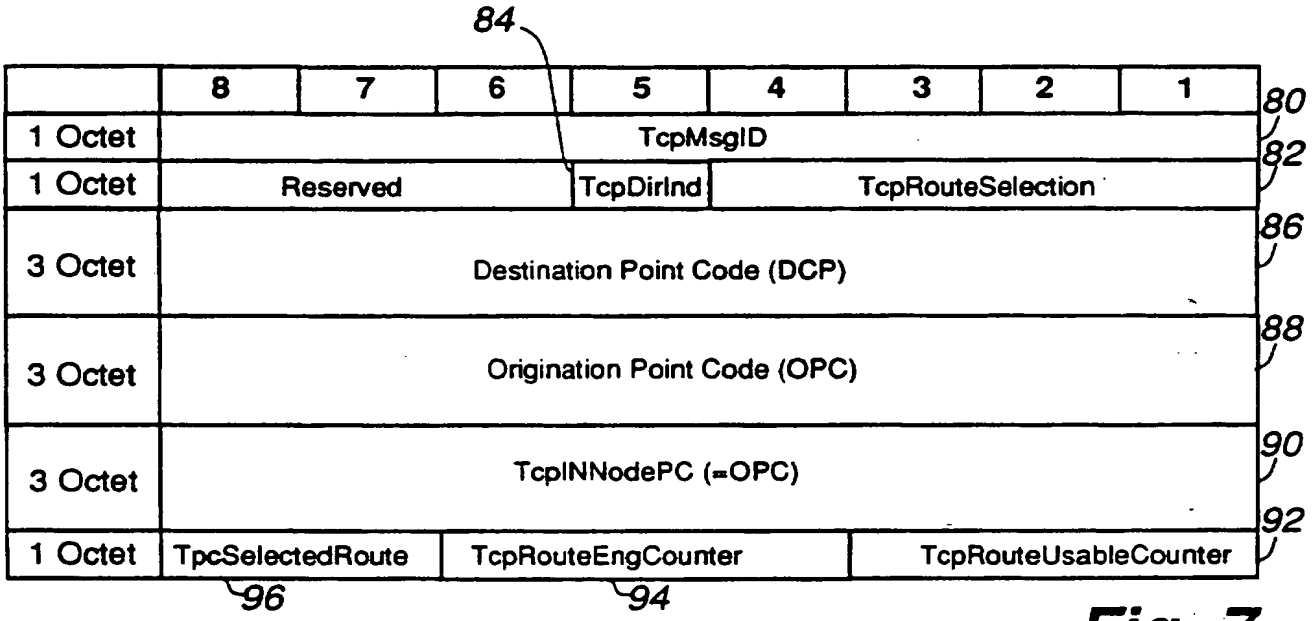


Fig. 7

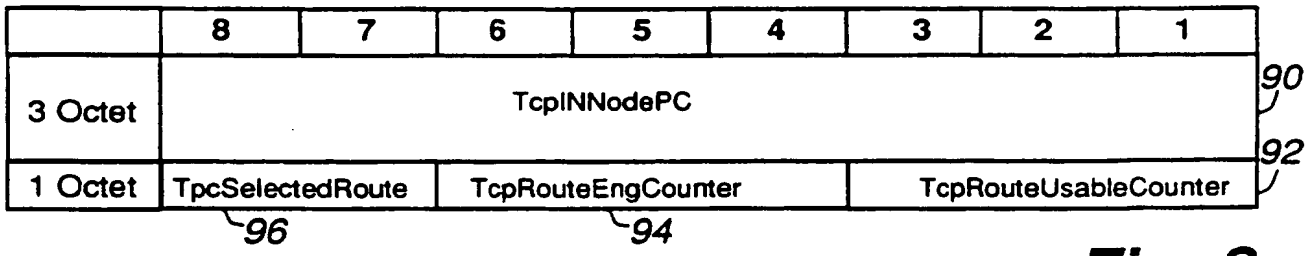


Fig. 8

	8	7	6	5	4	3	2	1
3 Octet	TcpINNodePC (=DPC)							
1 Octet	TpcSelectedRoute		TcpRouteEngCounter			TcpRouteUsableCounter		
3 Octet	TcpFirstLegEndPC							
1 Octet	TcpFaultCode							

90

98

100

Fig. 9

	8	7	6	5	4	3	2	1
3 Octet	TcpINNodePC							
1 Octet	TpcSelectedRoute			TcpCounter				
3 Octet	TcpFirstLegEndPC							
1 Octet	TcpFaultCode							

101

100

Fig. 10

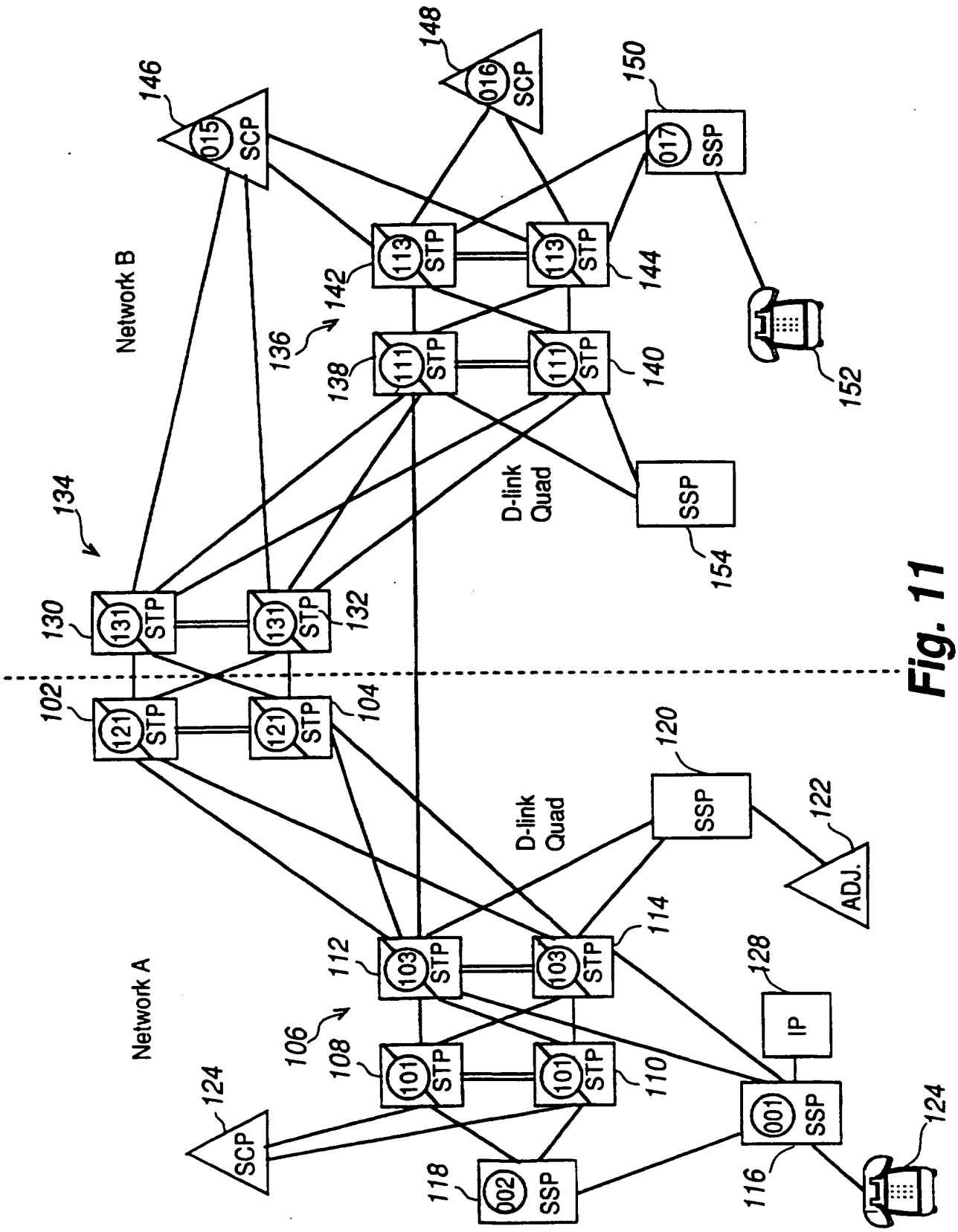

Network A
Network B
D-link Quad
D-link Quad
SCP
SSP
STP
IP
ADJ.
015
016
017
001
002
101
103
111
113
121
131
102
104
106
108
110
112
114
116
118
120
122
124
128
130
132
134
136
138
140
142
144
146
148
150
152
154

Fig. 11

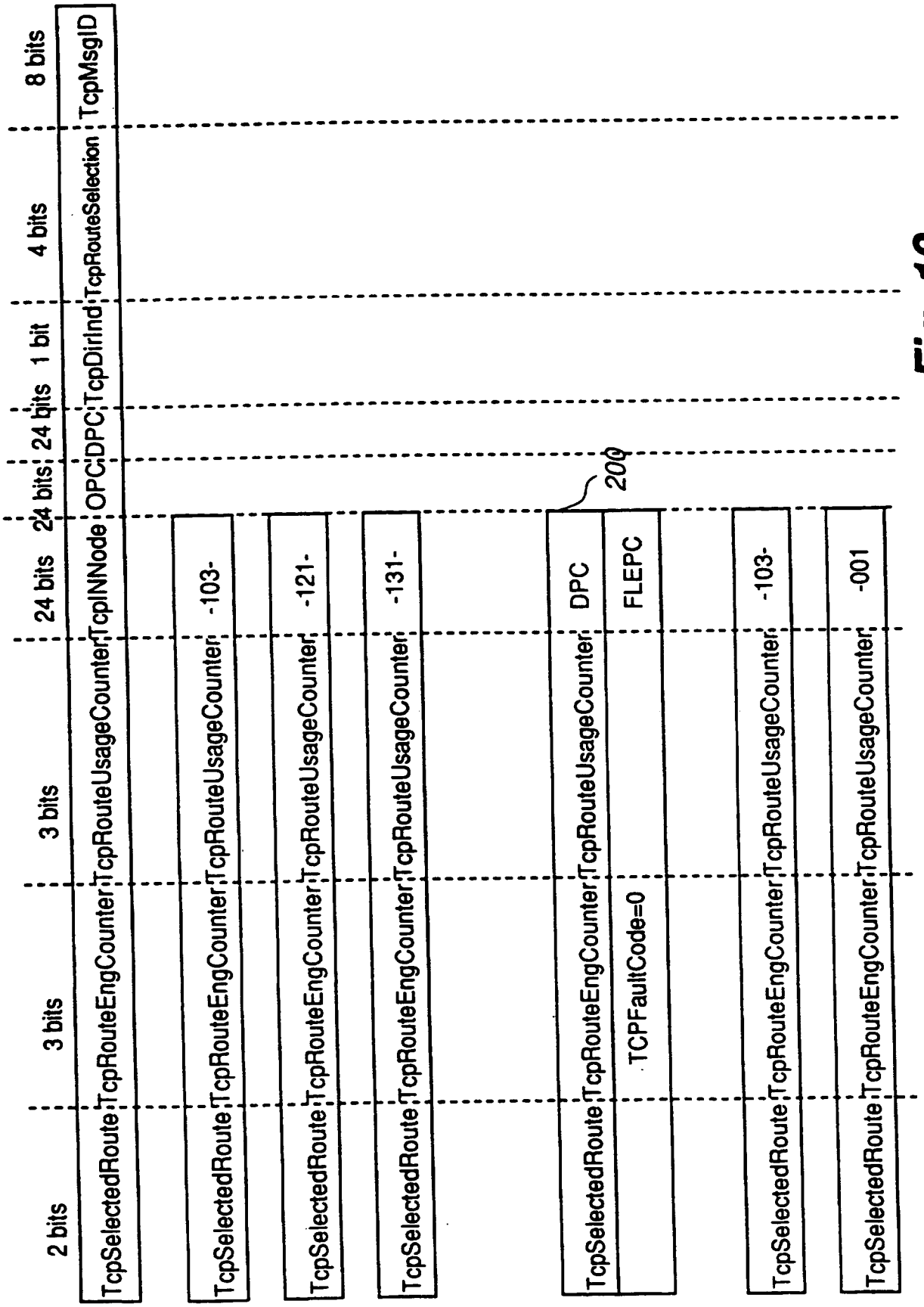

2 bits
3 bits
3 bits
24 bits
24 bits
24 bits
1 bit
4 bits
8 bits
TcpSelectedRoute
TcpRouteEngCounter
TcpRouteUsageCounter
TcplNNode
OPC
DPC
TcpDirInd
TcpRouteSelection
TcpMsgID
-103-
-121-
-131-
DPC
FLEPC
TCPFaultCode=0
-103-
-001
200

Fig. 12

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 95/00327

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q3/00 H04M3/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	NOMS 92-IEEE 1992- NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, vol. 3, 6 April 1992 - 9 April 1992 MEMPHIS(US), pages 709-720, MYRANDA A. JOHNSON ET AL 'NEW SERVICE TESTING FUNCTIONS FOR ADVANCED INTELLIGENT NETWORKS'	1,3-7,31
A	see abstract	16
Y	DE,B,12 89 884 (SIEMENS) 27 February 1969 see column 12, line 16 - line 57	1,3-7,31
A	EP,A,0 411 798 (A.T.T.) 6 February 1991 see abstract	
A	US,A,4 910 760 (REFORMATO) 20 March 1990	

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 August 1995	18. 09. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Vandevenne, M

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB,A,2 176 972 (ROBINTON PRODUCTS) 7 January 1987 see page 1, line 37 - page 2, line 60	
A	EP,A,0 214 398 (SIEMENS) 18 March 1987	
A	US,A,5 359 646 (JOHNSON ET AL) 25 October 1994 see column 16, line 52 - column 17, line 9	1,16

1

INTERNATIONAL SEARCH REPORT

information on patent family members

Int[illegible]nal Application No
PCT/CA 95/00327

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
DE-B-1289884		BE-A-	696239	29-09-67
		BE-A-	730660	29-09-69
		DE-A-	1487901	16-01-69
		DE-A-	1762056	16-04-70
		FR-A-	2005024	05-12-69
		FR-A-	1524235	11-09-68
		GB-A-	1176514	07-01-70
		GB-A-	1218902	13-01-71
EP-A-411798	06-02-91	US-A-	4959849	25-09-90
		CA-A,C	2017380	31-01-91
		DE-D-	69013789	08-12-94
		DE-T-	69013789	18-05-95
		ES-T-	2062379	16-12-94
		JP-A-	3066253	20-03-91
		JP-B-	6083315	19-10-94
US-A-4910760	20-03-90	NONE		
GB-A-2176972	07-01-87	US-A-	4692761	08-09-87
		BE-A-	904974	16-10-86
		CA-A-	1252535	11-04-89
		DE-A-	3619906	02-01-87
		FR-A-	2587570	20-03-87
		JP-A-	62048837	03-03-87
		NL-A-	8601614	16-01-87
		SE-A-	8602769	22-12-86
EP-A-214398	18-03-87	AU-B-	566499	22-10-87
		AU-A-	5982486	15-01-87
		CA-A-	1265227	30-01-90
		JP-C-	1600001	31-01-91
		JP-B-	2025318	01-06-90
		JP-A-	62064194	23-03-87
		US-A-	4797875	10-01-89
US-A-5359646	25-10-94	NONE		